(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 septembre 2002 (06.09.2002)

PCT

(10) Numéro de publication internationale
WO 02/069638 A1

(51) Classification internationale des brevets[7] :
H04N 7/167

(21) Numéro de la demande internationale :
PCT/IB02/00557

(22) Date de dépôt international :
25 février 2002 (25.02.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2001 0344/01 26 février 2001 (26.02.2001) CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRAVISION SA [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : CHAUBERT, Eric [CH/CH]; Vy-Creuse 9b, CH-1196 Gland (CH).

(74) Mandataire : LEMAN CONSULTING SA; Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: ENCRYPTION OF A COMPRESSED VIDEO STREAM

(54) Titre : ENCRYPTION D'UN FLUX VIDEO COMPRESSE

I 1	P/C 1-2	I 2	P/C 2-3	I 3

(57) Abstract: The purpose of the invention is to enable receipt of a compressed data stream through the use of powerful algorithms on terminals having weak cryptographic capabilities. The invention makes use of a method for encrypting a compressed video stream comprising independent data blocks and differential data blocks which consists in encrypting the independent data blocks and the differential data blocks according to a different level of encryption.

(57) Abrégé : Le but de la présente demande est de permettre la réception d'un flux de données compressée par l'utilisation d'algorithmes puissants sur des terminaux disposant de faibles capacités cryptographiques. Ce but est atteint par une méthode d'encryption d'un flux vidéo compressé, comprenant des blocs de données indépendantes et des blocs de données différentielles consistant à encrypter selon un niveau d'encryptage différent, les blocs de données indépendantes et des blocs de données différentielles.

WO 02/069638 A1

ENCRYPTION D'UN FLUX VIDEO COMPRESSE

La présente invention concerne une méthode visant encrypter un flux vidéo compressé, en particulier en permettant de renforcer le niveau de sécurité tout en ne pénalisant pas les ressources lors du décryptage.

Les algorithmes de compression vidéo sont basés sur le fait que généralement, les différences entre une image et sa suivante sont faibles et que l'expression des différences représente une quantité d'information bien plus réduite que l'image entière. Il a été observé que, d'une image à l'autre, un grand nombre d'informations ne changent pas, voire se retrouvent dans un plan légèrement différent.

Ce principe est appliqué dans des formats de type MPEG-2, MPEG-3, ou Quick Time.

Selon ces algorithmes, une première image, dite de référence est transmise au complet et une analyse des images suivantes est effectuée afin de déterminer et transmettre les différences. Selon la norme MPEG, on distingue les trames transmises intégralement (I-Frame) et les données différentielles de type MV (vecteur de déplacement) et de type DFD (différence entre le modèle MV et l'image réelle).

Selon les solutions connues, ces données sont ensuite encryptées selon un algorithme adapté au niveau de sécurité souhaité.

Afin de conserver une compatibilité lors de la transmission et du traitement, chaque ensemble est encrypté pour lui-même c'est-à-dire que l'attribut des trames demeure visible, seul le contenu est encrypté.

Avec l'évolution des moyens de stockage, il est courant de transmettre des données encryptées, représentant par exemple un film, vers l'unité d'un utilisateur.

Une fois le fichier stocké dans l'unité, un tiers peut avoir tout le temps nécessaire pour essayer de décrypter les données.

Afin de pallier ce risque, une première approche consiste à augmenter le niveau de sécurité sur le fichier, c'est-à-dire, d'utiliser des algorithmes puissants à clés longues.

Cette technique, bien que satisfaisante sur le plan de la sécurité, présente l'inconvénient d'imposer des ressources importantes à l'unité de décryptage.

La diversification des moyens de visualisation va dans le sens de l'utilisation des données par des unités disposant de faibles capacités cryptographiques. Ceci est le cas par exemple pour les nouveaux téléphones portables disposant d'un écran de visualisation. Pour ce type d'unité, l'utilisation en temps réel d'algorithmes sophistiqués n'est pas possible sans dégradation des performances de l'unité.

Ainsi, l'utilisation de blocs de données encryptés par des algorithmes puissants est incompatible avec une utilisation à destination de tous type d'unité d'utilisateurs.

Le but de la présente demande est donc de réconcilier l'utilisation d'algorithmes puissants avec des terminaux disposant de faibles capacités cryptographiques.

Ce but est atteint par une méthode d'encryption d'un flux vidéo compressé, comprenant des blocs de données indépendantes et des blocs de données

différentielles consistant à encrypter selon un niveau d'encryptage différent, les blocs de données indépendantes et des blocs de données différentielles.

Par bloc de données indépendantes, on entend des informations permettant d'obtenir le signal décompressé sans référence aux informations précédentes. Il peut s'agir par exemple des trames complètes (I-Frame).

Par bloc de données différentielles, on entend des informations permettant d'obtenir le signal décompressé par modification du signal précédent en appliquant ces informations différentielles.

En effet, cette solution permet de concentrer la sécurité maximale sur les informations indispensables à la décompression des images. Selon cette méthode, un premier algorithme est appliqué sur les trames complètes (I-Frame) du signal vidéo compressé et un second algorithme est appliqué aux informations différentielles de type MV et de type DFD.

Cette différence peut se faire également par l'utilisation de clés de longueur variable selon le type de données. Ainsi, les trames complètes seront encryptées par une clé de 2048 bits alors que les informations différentielles seront encryptées par une clé de 128 bits.

Selon une variante de l'invention, les informations différentielles ne sont pas encryptées.

Il est à noter que d'autres sources d'informations fonctionnant sur le principe différentiel, peuvent également utiliser cette méthode. C'est le cas par exemple pour la musique compressée selon le format MP3.

La présente invention sera mieux comprise à la lumière des dessins annexés, pris à titre non limitatifs, dans lesquels:

- la figure 1 illustre le flux compressé avant l'opération d'encryptage,
- la figure 2 représente le flux compressé sous forme encryptée,
- la figure 3 représente un flux compressé lors de sa transmission.

Sur la figure 1, le flux compressé est représenté par une suite de trames de type complète (I) et d'informations différentielles (P/C). Selon cet exemple, une première trame complète I 1, est suivie des trames P/C 1-2 permettant de reconstituer les trames successives entre la trame complète I 1 à la trame I 2.

De la même manière, la trame complète I 2 est suivie des trames successives différentielles P/C 2-3 permettant d'arriver à la trame complète I 3.

Ce flux est ensuite encrypté sélectivement selon le type de trame tel qu'illustré à la figure 2. Sur cette figure, on a utilisé une première clé k1 d'une longueur de 2048 bits pour encrypter les trames complète I 1, I 2 et I 3. Une seconde clé k2, par exemple de 128 bits, a été utilisée pour l'encryption des trames différentielles P/C 1-2 et P/C 2-3.

La longueur des clés k1 et k2 est donnée ici à titre indicatif et pourrait être de toute autre longueur.

Selon l'invention, la différence de qualité d'encryptage peut se faire au niveau des clés ou au niveau de l'algorithme utilisé. Ainsi, l'encryptage selon k1 représente par exemple un algorithme de type IDEA et l'encryptage selon la k2 représente un algorithme de type DES.

Lors de la diffusion de ce flux, les trames complètes sont envoyées en premier tel qu'illustré par la figure 3.

Cette particularité permet à l'unité réceptrice de débuter immédiatement le décryptage par les trames nécessitant un traitement long. Une fois ces trames décryptées, le traitement des trames différentielles peut se faire en temps réel du fait de l'exécution rapide du type d'algorithme choisi pour ces trames.

Selon une variante de l'invention, le niveau d'encryptage pour les trames complètes est différencier selon qu'il s'agit d'une première trame, telle que la trame I1, ou les trames suivantes (I2 et I3). En effet, pour bénéficier du signal décrypté et décompressé, il faut immédiatement traiter la première trame puis les trames de différences. C'est pourquoi, la première trame d'une série est encryptée avec un algorithme à décryption plus rapide que les trames complètes suivantes.

Cet algorithme peut être le même que pour les trames différentielles ou un autre algorithme.

REVENDICATIONS

1. Méthode d'encryption d'un flux vidéo compressé, comprenant des blocs de données indépendantes (I) et des blocs de données différentielles (P/C) caractérisé en ce qu'elle consiste à encrypter selon un niveau d'encryptage différent, les blocs de données indépendantes (I) et les blocs de données différentielles (P/C).

2. Méthode d'encryption d'un flux vidéo compressé selon la revendication 1, caractérisé en ce que les blocs de données indépendantes (I) sont encryptés par un algorithme de haut niveau alors que les blocs de données différentielles (P/C) sont encryptés par un algorithme à décryption rapide.

3. Méthode selon la revendication 1, caractérisé en ce que les blocs de données indépendantes (I) sont encryptés par une ou des clés longues, alors que les blocs de données différentielles (P/C) sont encryptés par une ou des clés courtes.

4. Méthode selon l'une des revendications 1 à 3, caractérisé en ce que, lors de la transmission du signal compressé, les blocs de données indépendantes (I) sont groupés par série, la méthode consistant à encrypter le premier bloc de cette série selon un niveau d'encryptage différent des blocs indépendants suivants.

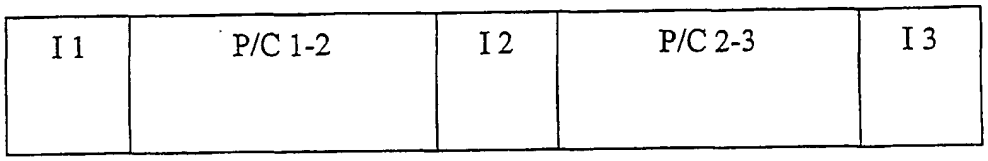

Fig 1.

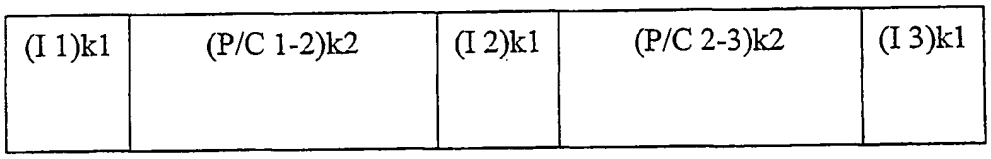

Fig 2.

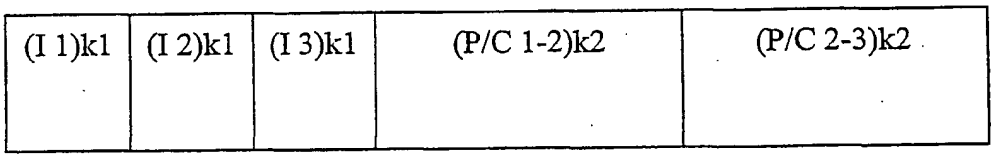

Fig 3.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 984 630 A (MINDPORT BV) 8 March 2000 (2000-03-08) page 2, column 1, line 52 -column 2, line 3 page 2, column 2, line 41 -page 3, column 4, line 4	1-3
A	US 5 838 791 A (TORII NAYOYA ET AL) 17 November 1998 (1998-11-17) column 4, line 7 -column 5, line 32	1-4

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 April 2002	23/04/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0984630 A	08-03-2000	EP 0984630 A1	08-03-2000
		JP 2000092045 A	31-03-2000
		ZA 9905259 A	21-02-2000
US 5838791 A	17-11-1998	JP 8056356 A	27-02-1996

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 984 630 A (MINDPORT BV) 8 mars 2000 (2000-03-08) page 2, colonne 1, ligne 52 -colonne 2, ligne 3 page 2, colonne 2, ligne 41 -page 3, colonne 4, ligne 4	1-3
A	US 5 838 791 A (TORII NAYOYA ET AL) 17 novembre 1998 (1998-11-17) colonne 4, ligne 7 -colonne 5, ligne 32	1-4

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
16 avril 2002	23/04/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

de internationale No
PCT/IB 02/00557

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0984630 A	08-03-2000	EP 0984630 A1	08-03-2000
		JP 2000092045 A	31-03-2000
		ZA 9905259 A	21-02-2000
US 5838791 A	17-11-1998	JP 8056356 A	27-02-1996